REMARKS

Claims 19-25 are pending in this application.

Claims 19-25 are rejected.

The office action dated February 2, 2006 indicates that base claim 19 is rejected under 35 USC §103(a) as being obvious over Sullivan U.S. Publication No. 2003/0093320 in view of Chopra U.S. Patent No. 6,510,509. Although claim 19 has been amended for clarity, this rejection is respectfully traversed.

Base claim 19 recites a secure transaction system comprising a plurality of servers for providing a web-based tax service that allows merchant subscribers to accumulate tax information. Base claim 19 also recites means for providing security for information on the servers and information during transmission between the servers.

Sullivan discloses a tax compliance transaction system 200 that receives transaction data from sellers and purchasers, and calculates tax liability information (paragraph 0005). Sullivan states the system 200 includes one or more processors that are centralized (see paragraph 5, line 7; paragraph 69, line 1; paragraphs 124-127; and Figure 1). The system 200 described at paragraph 124-127 is implemented in a personal computer.

Sullivan's system 200 can be implemented over multiple computers that are connected via a computer network (paragraph 130, lines 3-8). Paragraph 130 states that different "configurations of computers in a network permit many users to participate in a transaction, even if they are disbursed geographically." Paragraph 131 states modules shown in the figures can be implemented on different computers. However, it does not specify which modules. Paragraph 130 suggests that these modules relate to the users, so they can participate from

different geographic locations. Sullivan's paragraphs 130-131 do not teach or suggest that the different tax liability functions are performed by different servers.

Moreover, Sullivan does not describe a means for providing secure transmission of information between computers. Sullivan uses password access to prevent unauthorized sellers and purchases from gaining access to the system 200 (paragraph 40). However, the password access does not protect transmitted data after an authorized user has lawfully gained access. For example, it does not protect transmitted data against eavesdropping, connection hijacking, network-level virus attacks, etc.

Chopra's firewall does not provide security for information transmitted between computers. Chopra's firewall examines packets at a packet level and applies rules to the packets (col. 5, lines 50-54; col. 6, lines 53-59; col. 4, lines 33-45). However, Chopra does not teach or suggest rules that would provide security for information during transmission between servers. Chopra's firewall might protect the computers in a network, but not the information as it is being transmitted between the computers.

Sullivan does not teach or suggest that the network computers are servers. Paragraphs 130-131 describe computers, not servers. On page 3 of the office action, the examiner alleges that Sullivan's computers "must" be servers. However, the allegation is unsubstantiated. Sullivan does not impose such a requirement, nor does any other document made of record. If the allegation is based on the examiner's personal knowledge, the examiner should support the allegation with an affidavit pursuant to MPEP pursuant to MPEP §707 and 37 CFR §1.104(d)(2). If the examiner does not produce an affidavit or does not cite a document supporting the allegation, the examiner should withdraw the rejection for lack of evidence of obviousness.

Based on the evidence made of record, prima facie obviousness of base claim 19 has not been established. Therefore, the '103 rejection of base claim 19 should be withdrawn.

Sullivan and Chopra, alone and in combination, do not teach or suggest the managed firewalls of claim 21. The examiner has no factual basis to allege that Chopra's firewall prevents "unwanted data from being entered into the system while data is being transmitted between subscribers and the servers." Chopra's firewall inspects the IP address of packets. It does not examine the data within the packets.

Each of the features in claim 23 is known individually. However, none of the cited documents teach or suggest that these features can be combined to "provide security for information on the servers and information transmitted between the servers" of a secure transaction system that provides a web-based tax service. For example, none of the documents made of record teach or suggest a combination of "a tiered architecture, PKI 2-way authentication and authorization, HTTPS post, with XML document and SSH for remote administration" for providing security for information on the servers and information transmitted between the servers.

The office action appears to take official notice, not only of these individual features, but of the combination as well. Official notice of the combination is challenged. If the examiner want to allege that the combination is obvious, he will have to find evidence of obviousness in the prior art.

For the reasons above, claims 19-25 should be allowed over the combination of Sullivan and Chopra. The examiner is encouraged to contact applicants' attorney Hugh Gortler to discuss any issues that might remain.